

# Towards designing robust coupled networks

Christian M. Schneider,<sup>1,\*</sup> Nuno A. M. Araújo,<sup>1,†</sup> Shlomo Havlin,<sup>2,‡</sup> and Hans J. Herrmann<sup>1,3,§</sup>

<sup>1</sup>*Computational Physics for Engineering Materials, IfB,  
ETH Zurich, Schafmattstrasse 6, 8093 Zurich, Switzerland*

<sup>2</sup>*Minerva Center and Department of Physics, Bar-Ilan University, 52900 Ramat-Gan, Israel*

<sup>3</sup>*Departamento de Física, Universidade Federal do Ceará, 60451-970 Fortaleza, Ceará, Brazil*

In nature and technology, network-like systems are typically coupled and the resilience of one is affected by the others. The failure of a small fraction of elements in the system may have catastrophic effects, by triggering a cascade of events which drastically affects the global connectivity. We show that by choosing the proper autonomous nodes, catastrophic cascading failures can be avoided. We reveal that, when a small optimal fraction of autonomous nodes (about 10%) is properly selected the nature of the percolation transition changes from discontinuous to continuous and the robustness of the system is significantly improved. This is in contrast to random selection where close to 50% of autonomous nodes are needed. Surprisingly, even for coupled Poissonian type networks, where the variety between the node degrees is small, the proper choice of autonomous nodes leads to a large improvement.

PACS numbers: 89.75.Hc, 64.60.ah, 89.75.Da, 89.75.Fb

Complex networks have been crucial to understand the robustness of systems to failures or malicious attacks [1–3]. For theoretical simplicity, these systems have usually been considered to be isolated and independent of other network systems. However, in nature and technology systems are rather dependent and failures in one network are very likely to affect the others [4]. This coupling between systems has catastrophic effects on their robustness [5]. For example, the interdependency between power stations and local communication servers magnified the 2003 blackout in Italy and Switzerland [5, 6]. Also, the way banks are interconnected with insurance companies promoted a cascade effect in the recent financial crises [7, 8]. Understanding how to protect these systems and reduce their vulnerability is a question of paramount interest, which we address here.

Recently, a percolation framework has been proposed by Buldyrev *et al.* [5] to study the properties of fully interdependent networks. They considered a system of two networks, *A* and *B*, where each *A*-node is coupled to a *B*-node, via bi-directional links, such that when one node fails the other cannot function either. Due to such coupling, the failure of some nodes may trigger a domino effect where, not only its corresponding node in the other network fails, but also all nodes that become disconnected from the giant components of both networks fail. This causes further cascading failures in the system, yielding a discontinuous percolation transition. Parshani *et al.* [9] showed that the vulnerability of the system is reduced when decreasing the degree of coupling between nodes and, if only a significant fraction ( $\approx 0.5$ ) of nodes is decoupled, at a critical coupling, the system is significantly more robust and the transition changes from discontinuous to continuous. The coupling is reduced by selecting a certain fraction of nodes in the system which become independent of nodes in the other network. From

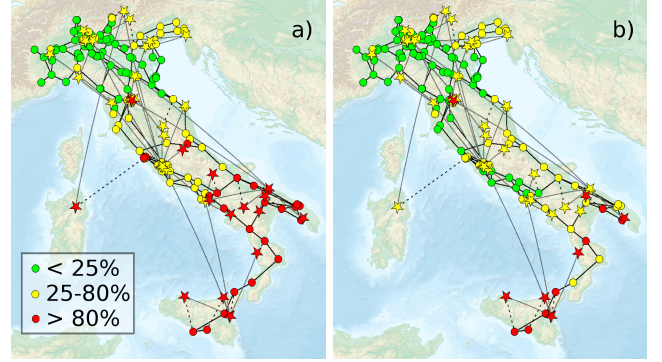


FIG. 1. (color online) Schematic representation of two coupled networks in Italy, the communication system (39 stars) and the power grid (310 circles) [6]. The coupling between the networks was established based on the geographical location of the nodes, such that each communication server is coupled with the closest power station. The color scheme stands for the probability that the node is inactive after the random failure of 14 communication servers. In a) all communication servers are coupled while in b) four servers have been decoupled following the strategy proposed here. A significant increase in the resilience of the system to failures can be obtained.

a technological point of view, this corresponds to creating autonomous nodes that do not depend on the other network. For example, if we consider the coupling between power stations and communication servers, autonomous power stations have alternative communication systems which are used when the communication servers fail. In the network of communication servers, a server is autonomous when it has its own emergency power supply which is independent of the power grid. The crucial open question that we pose and answer here, is how to choose these autonomous nodes in order to achieve high robustness. We propose a method, based on degree and cen-

trality, to identify these autonomous nodes that maximize the system robustness. We show that, with this scheme, the critical coupling increases, i.e., the fraction of nodes that needs to be decoupled to smoothen out the transition is much smaller (close to 0.1 compared to 0.5). Significant improvement is observed for different networks including the Erdős-Rényi graph (ER) that have a narrow degree distribution and such an improvement in the robustness was unexpected. In Fig. 1 we apply the proposed strategy to a real system in Italy [6] and show that by protecting only four nodes the robustness of the system is significantly improved (details in the figure caption).

We consider a pair of networks,  $A$  and  $B$ , randomly generated. A fraction  $q$  of the nodes in  $A$  are coupled with nodes in  $B$ , through inter-network links. In each network, nodes need to be connected to the largest component of their network to be functional. Initially, all nodes in each network are part of the largest component,  $q$  is the degree of coupling and  $1 - q$  is the fraction of autonomous nodes (not coupled via inter-network links). Due to the coupling, when one node in network  $A$  fails, or is attacked, the corresponding one in network  $B$  cannot function either. Consequently, all nodes bridged to the largest connected component through these nodes, together with their counterpart in the other network, become also deactivated. A cascade of failures occurs that can have drastic effects on the global connectivity [5, 9]. To analyze the response of the system to failures we follow its properties when  $A$ -nodes are sequentially attacked. At each iteration an  $A$ -node is randomly removed together with all affected ones. Failures are considered irreversible and all links from deactivated nodes are removed from the system. Notwithstanding the simplicity of solely considering random attacks, this model can be straightforwardly extended to targeted ones [10]. As explained in the *Supplemental Material* [11], to quantify the resilience of the system to random attacks we extend, to coupled systems, the definition of robustness  $R$  proposed for single networks in Ref. [2]. To demonstrate our method of selecting autonomous nodes, two ER graphs, with average degree four, have been coupled randomly with 10% of autonomous nodes. Under a sequence of random failures, the coupled system is fully fragmented when less than 50% of the nodes fail, as seen in Fig. 2. For a single ER, with the same average degree, the global connectivity is only lost after the failure of 75% of the nodes. Figure 2 also shows ((red-)dotted line) the case where the autonomous nodes in both networks are chosen as follows. Nodes in each network are ranked according to their betweenness, defined as the number of shortest paths between all pairs of nodes passing through these nodes [12, 13]. The first  $(1 - q)N$  nodes, the ones having the highest betweenness, are chosen as autonomous and the remaining ones are coupled randomly. With this strategy, the robustness,  $R$ , of the system is improved by

more than 10% and the corresponding increase of  $p_c$  is about 40%, from close to 0.5 to close to 0.7. Further improvement can be achieved if also the coupled nodes are paired according to their position in the ranking according to betweenness, corresponding to the (blue-)dashed line in Fig. 2. In that case, robustness is increased by 20% compared to the original case, since interconnecting similar nodes increases the global robustness [14, 15].

Two types of technological challenges are at hand: either a system has to be designed robust from scratch or it already exists and is constrained to a certain topology, but requires improved robustness. In the first case, the best procedure is to choose the nodes with highest betweenness in each network as autonomous and couple the others based on their position in the ranking according to betweenness. When the system already exists, rewiring is usually a time-consuming and expensive process, and mainly the creation of autonomous nodes may

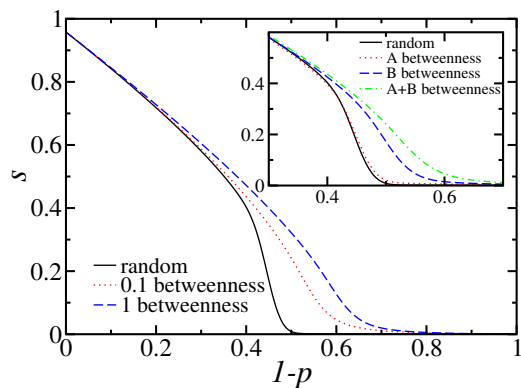


FIG. 2. (color online) Fraction of nodes in the largest connected cluster in network  $A$ ,  $s$ , as a function of the fraction of randomly removed nodes  $1 - p$ , for two coupled ER (average degree four) with 90% of the nodes connected by inter-network links ( $q = 0.9$ ), showing that robustness can significantly be improved by properly selecting the autonomous nodes. The (black-)solid line corresponds to randomly interconnected graphs with the 10% autonomous nodes randomly chosen. For the (red-)dotted line the autonomous nodes are chosen as the ones with highest betweenness. For the (blue-)dashed curve, the nodes in both networks were ranked according to their betweenness, where the first 10% were considered autonomous and the following 90% inter-connected according to their position in the ranking. Due to the finite size, the discontinuous nature of the solid curve is hardly visible in the plot. In the inset, we start with two fully interconnected ER. 10% of their nodes are decoupled according to three different strategies: randomly ((black-)solid line), the ones with highest betweenness in network  $A$  ((red-)dotted line), and the ones with highest betweenness in network  $B$  ((blue-)dashed line). The (yellow-)dotted-dashed line is only for sake of comparison and corresponds to the (red-)dotted line in the main plot. Results have been averaged over  $10^2$  configurations of two networks with  $10^3$  nodes each. For each configuration we averaged over  $10^3$  sequences of random attacks.

be economically feasible. The simplest procedure consists in choosing as autonomous both nodes connected by the same inter-network link. However, in general, the betweenness of coupled nodes are not correlated. An  $A$ -node with high betweenness may not, necessarily be, inter-connected with a high betweenness  $B$ -node. In the inset of Fig. 2 we compare between choosing the autonomous pairs based on the betweenness of the node in network  $A$  or in network  $B$ . The curves for random selection and for the most efficient design are both included for reference. When pairs of nodes are picked based on the ranking of betweenness in the network under the initial failure (network  $A$ ), the robustness almost does not improve compared to choosing randomly. If, on the other hand, network  $B$  is considered for autonomous high betweenness nodes, the robustness is improved by more than 15%, revealing that the protection scheme is significantly more efficient in this case. This asymmetry between  $A$  and  $B$  network is due to the fact that we attack only nodes in network  $A$ , triggering the cascade, that initially shuts down the corresponding  $B$ -node. The betweenness is related to the number of nodes which become disconnected from the main cluster and consequently affect back the network  $A$ . Therefore, the control of the betweenness of  $B$ -nodes which may be affected is a key mechanism to downsize the cascade. On the other hand, when a high-betweenness node is protected in network  $A$  it can still be attacked since the initial attack does not distinguish between autonomous and non-autonomous nodes.

In Fig. 3(a) we plot the robustness of two coupled ER for different  $q$ . Four different criteria to select the autonomous nodes in both networks are compared: betweenness, degree,  $k$ -shell, and random choice. In the degree strategy, the selected nodes to be autonomous are the ones with highest degree. In the  $k$ -shell strategy, the nodes with the highest  $k$ -shell in the  $k$ -shell decomposition are chosen [16]. The remaining nodes, for all cases, have been randomly inter-linked. In the inset, we see the relative robustness for the first three methods when compared to the random case,  $R/R_{\text{random}}$ . Since ER are characterized by a small number of  $k$ -shells, the  $k$ -shell decomposition is less efficient than the random strategy for some values of  $q$ . The significantly improved robustness for the betweenness strategy compared to the random case is evident. While in the random case, for  $q \gtrsim 0.4$ , a significant decrease of the robustness with  $q$  is observed, in the betweenness case, the change is smoother and significantly drops only for higher values of  $q$ . A maximum in the ratio  $R/R_{\text{random}}$  occurs for  $q \approx 0.85$ , where the relative improvement is above 12%. Since in random networks, the degree of a node is strongly correlated with its betweenness [13], their results are similar. As shown in the *Supplemental Material* [11], for modular networks [17] where the correlation between degree and betweenness is lower, the best strategy to select au-

tonomous nodes is based on the betweenness. Also for random regular graphs, where all nodes have the same degree, we find improvements when choosing betweenness.

Many real-world systems are characterized by a degree distribution which is scale free with a degree exponent  $\gamma$  [1, 18]. In Fig. 3(b) we plot  $R$  as a function of  $q$  for two coupled scale-free networks (SF) with  $10^3$  nodes each and  $\gamma = 2.5$ . Similar to the two coupled ER, this system is also significantly more resilient when the autonomous nodes are selected to be the ones with highest betweenness. For values of  $q \lesssim 0.85$  the robustness of the coupled system is similar to that of a single network ( $q = 0$ ) since the most relevant nodes in the system are decoupled. A peak in the relative robustness,  $R/R_{\text{random}}$  (see inset of Fig. 3b), occurs for  $q \approx 0.95$  where the improvement, compared to the random case, is almost 30%. Betweenness, degree, and  $k$ -shell, have similar impact on the robustness since these three properties are strongly correlated for SF. From Fig. 3 and from the *Supplemen-*

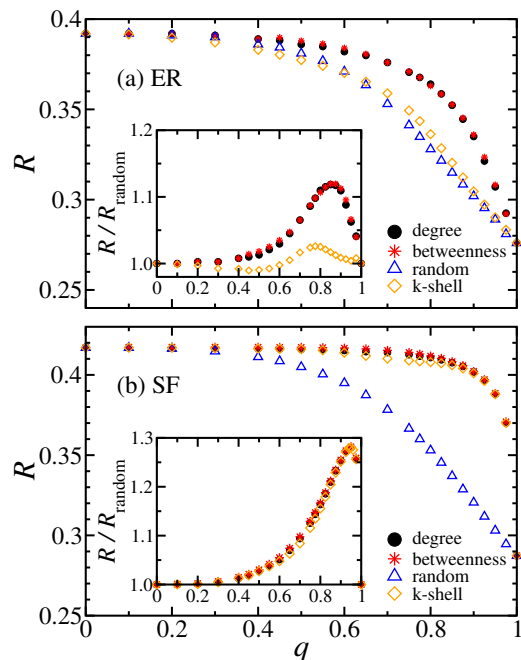


FIG. 3. (color online) Dependence of the robustness,  $R$ , on the degree of coupling,  $q$ , for two, interconnected, (a) ER (average degree four) and (b) SF with degree exponent  $\gamma = 2.5$ , revealing that, when our proposed strategy is applied, the optimal fraction of autonomous nodes is relatively very small. Autonomous nodes are chosen in four different ways: randomly ((blue-)triangles), high degree ((black-)dots), high betweenness ((red-)stars), and high  $k$ -shell ((yellow-)rhombi). The insets show the relative improvement of the robustness, for the different strategies of autonomous selection compared with the random case. Results have been averaged over  $10^2$  configurations of two networks with  $10^3$  nodes each. For each configuration we averaged over  $10^3$  sequences of random attacks.

*tal Material* [11], we see that, for both SF and ER, the robustness of the system is significantly improved by decoupling, based on the betweenness, less than 15% of the nodes. Studying the dependence of the robustness on the nodes average degree we conclude that for average degree larger than five, even 5% autonomous nodes are enough to achieve more than 50% of the maximum possible improvement.

The vulnerability of the system is strongly related to the degree of coupling,  $q$ . Parshani *et al.* [9] have analytically and numerically shown that, at a critical coupling  $q = q_c$ , the transition changes from continuous (for  $q < q_c$ ) to discontinuous (for  $q > q_c$ ). The effect of our proposed scheme on  $q_c$  is shown in Fig. 4, where the number of iterations (NOI) [5, 15] in the cascade is plotted for coupled ER, with  $q = \{0.9, 0.95\}$  and autonomous nodes selected either randomly or according to their betweenness. The peak of the NOI represents the percolation threshold  $p_c$ . If the NOI at  $p_c$  increases with the system size, the transition is discontinuous. For  $q = 0.95$ , a peak (representing  $p_c$ ) is observed with both strategies, but being significantly smaller for the betweenness. For  $q = 0.9$ , the peak is undetectable for betweenness, i.e., attacks on  $A$ -nodes produce very few cascades. In the inset, we show, for different system sizes, how the maximum of NOI depends on the coupling. While for low  $q$  the maximum shows no system size dependence, a sign of a continuous transition [15], for  $q > q_c$  the transition

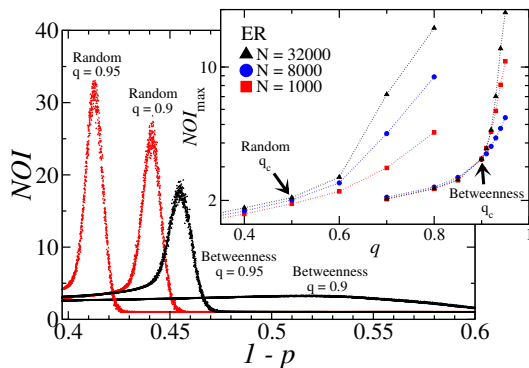


FIG. 4. (color online) Number of iterations (NOI) in the cascade as a function of the fraction of removed nodes  $1 - p$ , demonstrating that when betweenness is considered the large cascade can be suppressed. Two coupled ER (average degree four) have been considered with  $N$  nodes each. For the main plot  $N = 32000$  and  $q = \{0.9, 0.95\}$ . Autonomous nodes have been picked randomly in the left (red) and according to their betweenness for the two peaks in the right (black). In both cases, all other nodes have been coupled randomly. In the inset, we show the maximum NOI for different system sizes, as a function of  $q$ , for the random and the betweenness cases. The arrows point to the position where the transition changes from continuous to discontinuous. Results have been averaged over  $10^2$  configurations and  $10^3$  sequences of random attacks for each one.

becomes discontinuous since the maximum scales with the system size. For random selection  $q_c \sim 0.5$ , whilst for the strategy based on the betweenness  $q_c \gtrsim 0.9$ , i.e., in the latter case decoupling only 10% of the nodes is enough to change the nature of the transition from discontinuous to continuous. The same is observed for SF and when autonomous nodes are selected based on the degree. Therefore, the proposed strategy significantly improves the robustness of the system and with a relatively small amount of autonomous nodes the transition is softened by avoiding large cascades.

In summary, we propose a method to choose the autonomous nodes in order to optimize the robustness of coupled systems to failures. We find the betweenness and the degree to be the key parameters for the selection of such nodes and we show that for modular networks the former is the most effective one. Considering the real case of the Italian communication system coupled with the power grid, we show that protecting the four communication servers with highest betweenness improves the robustness of the system and reduces the chances of catastrophic failures, like the blackout of 2008. When this strategy is implemented the resilience of the system to random failures or attacks is significantly improved and the fraction of autonomous nodes necessary to change the nature of the percolation transition, from discontinuous to continuous, is significantly reduced. We also show that, even for networks with a narrow diversity of nodes, like Erdős-Rényi graphs, the robustness of the system can be significantly improved by properly peaking a small fraction of nodes to be autonomous.

We acknowledge financial support from the ETH Competence Center Coping with Crises in Complex Socio-Economic Systems (CCSS) through ETH Research Grant CH1-01-08-2. We thank the Brazilian agencies CNPq, CAPES and FUNCAP, and the grant CNPq/FUNCAP. SH acknowledges the European EPIWORK project, the Israel Science Foundation, ONR, DFG, and DTRA.

\* schnechr@ethz.ch

† nuno@ethz.ch

‡ havlin@ophir.ph.biu.ac.il

§ hans@ifb.baug.ethz.ch

- [1] R. Albert *et al.*, *Nature*, **406**, 378 (2000); A. L. Lloyd and R. M. May, *Science*, **292**, 1316 (2001); F. Liljeros *et al.*, *Nature*, **411**, 907 (2001); V. Colizza, A. Barrat, M. Barthélemy, and A. Vespignani, *P. Natl. Acad. Sci. USA*, **103**, 2015 (2006).
- [2] C. M. Schneider *et al.*, *Proc. Nat. Acad. Sci.*, **108**, 3838 (2011).
- [3] R. Cohen *et al.*, *Phys. Rev. Lett.*, **85**, 4626 (2000); **86**, 3682 (2001); D. S. Callaway *et al.*, *ibid.*, **85**, 5468 (2000); L. K. Gallos *et al.*, *ibid.*, **94**, 188701 (2005); P. Holme *et al.*, *Phys. Rev. E*, **65**, 056109 (2002).
- [4] J. Peerenboom *et al.*, *Pro. CRIS/DRM/IIIT/NSF Work-*

- shop Mitigat. Vulnerab. Crit. Infrastruct. Catastr. Failures (2001).
- [5] S. V. Buldyrev *et al.*, Nature, **464**, 1025 (2010).
  - [6] V. Rosato *et al.*, Int. J. Crit. Infrastruct., **4**, 63 (2008).
  - [7] F. Schweitzer *et al.*, Science, **325**, 422 (2009).
  - [8] S. Havlin *et al.*, arXiv:1012.0206.
  - [9] R. Parshani *et al.*, Phys. Rev. Lett., **105**, 048701 (2010).
  - [10] X. Huang *et al.*, Phys. Rev. E, (in press, 2011).
  - [11] See Supplemental Material at.
  - [12] R. Cohen and S. Havlin, *Complex networks: structure, robustness and function* (Cambridge University Press, United Kingdom, 2010).
  - [13] M. E. J. Newman, *Networks: An Introduction* (Oxford University Press, Oxford, 2010).
  - [14] S. V. Buldyrev *et al.*, Phys. Rev. E, **83**, 016112 (2011).
  - [15] R. Parshani *et al.*, EPL, **92**, 68002 (2010).
  - [16] S. Carmi *et al.*, Proc. Natl. Acad. Sci. USA, **104**, 11150 (2007).
  - [17] E. Ravasz *et al.*, Science, **297**, 1551 (2002); B. L. M. Happel and J. M. J. Murre, Neural Netw., **7**, 985 (1994); M. C. González *et al.*, Physica A, **379**, 307 (2007); K. A. Eriksen *et al.*, Phys. Rev. Lett., **90**, 148701 (2003).
  - [18] A. Clauset *et al.*, SIAM Rev., **51**, 661 (2009).



## Supplemental Material: Towards designing robust coupled networks

Christian M. Schneider,<sup>1,\*</sup> Nuno A. M. Araújo,<sup>1,†</sup> Shlomo Havlin,<sup>2,‡</sup> and Hans J. Herrmann<sup>1,3,§</sup>

<sup>1</sup>Computational Physics for Engineering Materials, IfB,  
ETH Zurich, Schafmattstrasse 6, 8093 Zurich, Switzerland

<sup>2</sup>Minerva Center and Department of Physics, Bar-Ilan University, 52900 Ramat-Gan, Israel

<sup>3</sup>Departamento de Física, Universidade Federal do Ceará, 60451-970 Fortaleza, Ceará, Brazil

### ROBUSTNESS

For single networks, different measures have been considered to quantify the robustness of the system to failures. Recently, it has been proposed to quantify the robustness  $R$  of such systems as

$$R = \frac{1}{N} \sum_{Q=1}^N S(Q) \quad , \quad (1)$$

where  $Q$  is the number of node failures,  $S(Q)$  the size of the largest connected cluster in a network after  $Q$  failures, and  $N$  is the total number of nodes in the network [1]. This definition corresponds to the area under the curve of the fraction of nodes, in the largest connected cluster, as a function of the fraction of failed nodes (shown in Fig. 2 of the Letter). Here we extend this definition to coupled systems by performing the same measurement, given by Eq. (1), only on the network where the random failures occur, namely, network  $A$  in the Letter.

### MODULAR NETWORKS AND RANDOM REGULAR GRAPHS

For the cases discussed in the Letter, results obtained by selecting autonomous nodes based on the highest degree do not significantly differ from the ones based on the highest betweenness. This is due to the well known finding that for Erdős-Rényi and scale-free networks, the degree of a node is strongly correlated with its betweenness [2]. However, many real networks are modular, i.e., composed of several different modules interconnected by less links, and then nodes with higher betweenness are not, necessarily, the ones with the largest degree [3]. Modularity can be found, for example, in metabolic systems, neural networks, social networks, or infrastructures [4–7]. In Fig. 1 we plot the robustness of the system for two coupled modular networks. Each modular network was generated from a set of four Erdős-Rényi networks, of 500 nodes each and average degree five, where an additional link was randomly included between each pair of modules. For a modular system, the nodes with higher betweenness are not necessarily the high-degree nodes but the ones bridging the different modules. Figure 1 shows that the strategy based on the betweenness emerges as better compared to the high degree method.

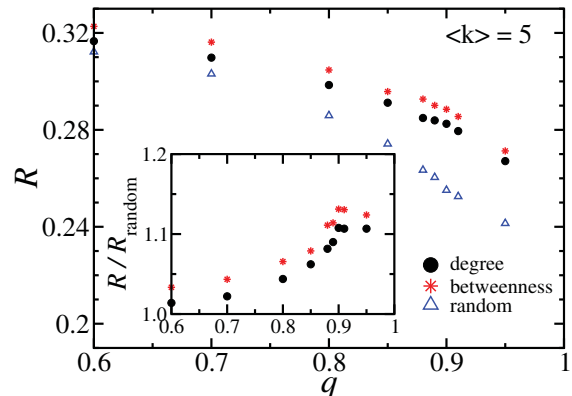


FIG. 1. Dependence of the robustness,  $R$ , on the degree of coupling,  $q$ , for two, randomly interconnected modular networks with  $2 \cdot 10^3$  nodes each. The modular networks were obtained from four Erdős-Rényi networks, with 500 nodes each and average degree five, by randomly connecting each pair of modules with an additional link. Autonomous nodes are selected in three different ways: randomly (blue triangles), higher degree (black dots), and higher betweenness (red stars). In the inset we see the relative enhancement of the robustness, for the second and third schemes of autonomous selection compared with the random case. Results have been averaged over  $10^2$  configurations and  $10^3$  sequences of random attacks to each one.

Another example that shows that betweenness is superior to degree is when we study a system of coupled random regular graphs. In random regular graphs all nodes have the same degree and are connected randomly. Figure 2 shows the dependence of the robustness on the degree of coupling, for two interconnected random regular graphs with degree 4. The autonomous nodes are selected randomly (since all degrees are the same) or following the betweenness strategy. Though all nodes have the same degree and the betweenness distribution is narrow, selecting autonomous nodes based on the betweenness is always more efficient than the random selection. Thus, the above two examples suggest that betweenness is a superior method to choose the autonomous nodes compared to degree.

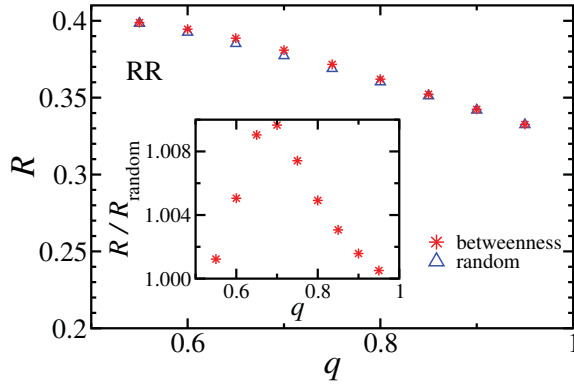


FIG. 2. Dependence of the robustness,  $R$ , on the degree of coupling,  $q$ , for two, randomly interconnected regular graphs with  $8 \cdot 10^3$  nodes each, all with degree 4. Autonomous nodes are selected in two different ways: randomly (blue triangles) and higher betweenness (red stars). In the inset the relative enhancement of the robustness, for the betweenness compared with the random case, is shown. Results have been averaged over  $10^2$  configurations and  $10^3$  sequences of random attacks to each one.

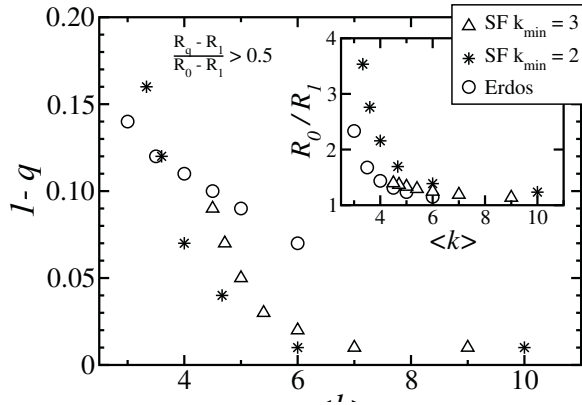


FIG. 3. Dependence on the average degree of the fraction of decoupled nodes ( $1 - q$ ) above which the improvement in the robustness of the system  $R_q - R_1$  is larger than 50% of the maximum improvement  $R_0 - R_1$ , where  $R_q$  is the robustness of the system with degree of coupling  $q$ . Two coupled networks have been considered with 8000 nodes each ( $10^2$  configurations with  $10^3$  sequences of random attacks to each one) and autonomous nodes were picked based on the betweenness. Triangles and stars correspond to scale-free networks with minimum degree three and two, respectively, and circles are for two Erdős-Rényi graphs. The inset, shows the relative robustness of the decoupled system  $R_0$  compared with the fully coupled one  $R_1$ . When autonomous nodes are selected based on the betweenness a significant improvement in the robustness of the system is obtained by solely decoupled less than 15% of the nodes. The larger the average degree the lower the fraction of decoupled nodes required to obtain such improvement.

### ROBUSTNESS IMPROVEMENT

For two coupled networks, the maximum robustness  $R_0$  is achieved when both are completely decoupled ( $q = 0$ ),

such that nodes in one are not affected by the other. On the other hand, the most vulnerable case, corresponds to a fully coupled system ( $q = 1$ ) with robustness  $R_1$ . For a certain degree of coupling  $q$ , we define the relative improvement as the ratio between the improvement  $R_q - R_1$  and the maximum possible improvement  $R_0 - R_1$ . Figure 3 shows the dependence on the average degree of the fraction of nodes that need to be autonomous to guarantee a relative improvement of more than 50%. Three types of systems have been considered, namely, coupled scale-free networks with minimum degree three and two, as well as coupled Erdős-Rényi graphs with different average degrees. For all considered cases, when autonomous nodes are selected based on the betweenness, a significant improvement is obtained by solely decoupling less than 15% of the nodes. The fraction of decoupled nodes to obtain such improvement in the robustness significantly decreases with the average degree. In the inset we see the ratio between the robustness of the fully independent ( $q = 0$ ) and dependent system ( $q = 1$ ) as a function of the average degree showing that this ratio goes to unity as expected since a large average degree corresponds to fully independent networks. This is since when the degrees are high a failure in one network will make a similar failure in the second network with little cascading failures.

\* schnechr@ethz.ch

† nuno@ethz.ch

‡ havlin@ophir.ph.biu.ac.il

§ hans@ifb.baug.ethz.ch

- [1] C. M. Schneider, A. A. Moreira, J. S. Andrade Jr., S. Havlin, and H. J. Herrmann, *Proc. Nat. Acad. Sci.*, **108**, 3838 (2011); H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade Jr., and S. Havlin, *J. Stat. Mech.*, P01027 (2011).
- [2] M. E. J. Newman, *Networks: An Introduction* (Oxford University Press, Oxford, 2010).
- [3] R. Cohen and S. Havlin, *Complex networks: structure, robustness and function* (Cambridge University Press, United Kingdom, 2010).
- [4] E. Ravasz, A. L. Somera, D. A. Mongru, Z. N. Oltvai, and A.-L. Barabási, *Science*, **297**, 1551 (2002).
- [5] B. L. M. Happel and J. M. J. Murre, *Neural Netw.*, **7**, 985 (1994).
- [6] M. C. González, H. J. Herrmann, J. Kertész, and T. Vicsek, *Physica A*, **379**, 307 (2007).
- [7] K. A. Eriksen, I. Simonsen, S. Maslov, and K. Sneppen, *Phys. Rev. Lett.*, **90**, 148701 (2003).